enterprise privacy office

Ransomware: Avoid Paying Up - Back Up!

» A significant threat to data privacy and security comes in the form of "ransomware." Ransomware is a type of malicious software designed to block system access until a sum of money is paid, or certain action is taken. Even if you pay or take the requested action, there's no guarantee the person or organization holding your data hostage will ever grant access.

WHAT DOES RANSOMWARE DO?

- Prevent you from accessing your computer network or files;
- Encrypt files so you can't use them; and
- Stop certain apps, like your web browser, from running.

WHAT IS THE BEST DEFENSE AGAINST THIS THREAT?

Back up your data every day and, prior to an emergency, test the back ups to ensure restoration is effective. By doing so, you take away the power of ransomware. If you become infected, just restore your data from the back up.

HOW CAN I REDUCE THE LIKELIHOOD OF BECOMING A VICTIM?

- Be aware of phishing emails and think twice before clicking on links, especially in unsolicited emails.
  - It's easy to forge the "from" address of an email. If an email appears to be from someone you know, but doesn't look quite right, don't click links or open attachments. Contact the sender and verify they sent the email.
  - If an email asks you to update your details, use caution and think before clicking on the link provided.
  - Don't open attachments to an email you weren't expecting or that was sent from someone you don't know.
- Visit only trusted websites and links provided by known sources.
- Use strong passwords that cannot be easily guessed.
- Follow information security policies and best practices.
  - Ensure anti-virus software is up-to-date.
  - Enable automated patches for operating systems and web browsers.
  - Ensure you have installed an up-to-date, real-time security product.

ADDITIONAL RESOURCES

- For technical guidance, the Division of Information Security (DIS) has issued Ransomware Update Advisory Number: 20160810A.
- The U.S. Department of Health and Human Services (HHS) warns that the FBI has reported an increase in ransomware attacks. For HIPAA-covered entities, HHS has issued guidance to help you understand and respond to the threat of ransomware. To view this guidance, please visit http://www.hhs.gov/blog/2016/07/11/your-money-or-your-phi.html.

PRIVACY POWER-UP

WHAT ARE PRIVACY POWER-UPS?

- Tips to ***ENERGIZE*** privacy program Implementation.
- Pointers on information privacy safeguards, training techniques, and compliance activities.
- Synopses of privacy hot topics, research, and technologies.
- Tools for agency privacy liaisons to increase privacy awareness and establish information privacy protections.

admin
THE SOUTH CAROLINA DEPARTMENT of ADMINISTRATION